DEPLOYING 802.11b WIRELESS NETWORKING WITHIN KETS

With the growing availability of standards-based 802.11b wireless network components, wireless networks are becoming a key element of the enterprise network. 802.11b networks enhance existing wired networks by providing convenient access to network resources for teachers/students carrying portable computers and handheld device. A wireless network can also provide a cost-effective alternative to relocating physical Ethernet jacks in environments where facilities are moved or changed frequently.

NETWORK DESIGN

Successful deployment of an 802.11b network requires careful planning and network design. This process includes determining network applications, coverage requirements, and number of users, client device types, and equipment selection. In addition, unlike wired networks, planners must assess environmental obstacles that can impede radio frequency (RF) signal transmissions.

In a heterogeneous wireless networking environment, it is important to select 802.11b standards-based wireless products that are interoperable. The main measure of 802.11b equipment interoperability is the Wireless Fidelity (Wi-Fi) certification program. Administered by the industry group, Wireless Ethernet Compatibility Alliance (WECA), the Wi-Fi logo on a product certifies its interoperability with other products containing the logo.

The Wi-Fi interoperability program tests for association and roaming capabilities, throughput, and required features such a 64-bit encryption. WECA tracks standards developments and enhances the interoperability testing to reflect these advancements.

Some vendors differentiate their 802.11 products with additional features. Some are options in the 802.11 standard such as 128-bit encryption, and some are proprietary features such as security/authentication schemes, roaming capabilities, key management, and Power over Ethernet.

Using or enabling proprietary extensions usually requires that a single vendor supply the wireless equipment, including Access Points and network cards. Proprietary extensions are not suitable for heterogeneous environments with a mix of hardware. Although the extensions provide specific benefits, they limit future flexibility. Before choosing to implement these features, it is important to assess the environment in which the wireless LAN will be used.

The first step in designing a wireless network is to determine the requirements of the network. This includes identifying the areas that need to be covered, the number of users and the types of devices they will use, applications, environment, and so forth. From these requirements, network designers can begin to determine how many Access Points are required and where they must be placed. The goal is to ensure adequate RF coverage

to stationary and roaming users of the wireless network. A key activity of this design process is to perform a site survey to determine the required coverage; number, density, and locations of Access Points; number of users; and channel selections. In addition, the site survey can identify conditions that inhibit performance through path and multipath loss, as well as RF interference.

Path loss refers to the loss of signal power experienced between the Access Point and the client system as the distance between the two increases. Transmission distance, obstacles such as walls, ceilings, and furniture, and the frequency of the transmission affect path loss. Generally, the higher the frequency of the signal, the shorter the transmission that can be achieved.

Multipath loss occurs as an RF signal bounces off objects in the environment such as furniture and walls while en route to its destination. The result is that an RF signal can take more than one path, arriving as multiple signals at its destination. This can impact performance significantly. Correct network design and the use of Access Points and client network interface controllers with antenna diversity help to correct for multipath loss.

RF interference is caused by other RF sources that also operate in the 2.4 GHz frequency band. These sources can include microwave ovens and cordless phones.

Access Point placement is typically determined using a combination of theoretical principles and a thorough site survey. The site survey uses building plans and physical site tours to identify optimal placement of Access Points. The resulting plan should take into account usage patterns and adverse conditions that can impact performance. Under good conditions, an Access Point can provide coverage up to approximately 150 feet indoors. An example of an environment where this distance could be achieved is a relatively open environment with high ceilings and no hard-wall offices or other impediments to the RF signal. In this environment, the Access Point can be placed high to provide an unimpeded signal to the wireless clients. In office environments with walls (including cube walls) and other impediments, a more typical range is 75-80 feet. Please note that these measurements are subject to change with advances in antennas.

Once the Access Points are installed, IT personnel can test the implementation by roaming the premises with a laptop and observing variations in signal strength. A poor signal or poor throughput at a particular location would be an indication that an adjustment in Access Point placement, density, or channel selection is required.

SECURITY DESIGN

Security mechanisms in 802.11b networks should be equivalent to existing mechanisms in wire-based networks. Wired network jacks are located in buildings already secured from unauthorized access through the use of keys, badge access, and so forth. A user must gain physical access to the building in order to plug a client computer into a network jack. In contrast, a wireless Access Point that is configured incorrectly may be

accessed from off the premises (for instance, from a parking lot adjacent to the building). Properly designed wireless networks secure access to the Access Points and isolate the Access Points from the internal private network prior to user authentication into the network domain.

There are three basic methods to secure access to an Access Point that are built into 802.11 networks:

- Service set identifier (SSID)
- Media Access Control (MAC) address filtering
- Wired Equivalent Privacy (WEP)

One or all of these methods may be implemented, but all three together provide the most secure solution.

Network access control can be implemented using an SSID associated with an Access Point or a group of Access Points. The SSID provides a mechanism to "segment" a wireless network into multiple networks serviced by one or more Access Points. Each Access Point is programmed with an SSID corresponding to a specific wireless network. To access this network, client computers must be configured with the correct SSID. A building might be segmented into multiple networks by floor or department. Typically, a client computer can be configured with multiple SSIDs for users who require access to the network from a variety of different locations.

Because a client computer must present the correct SSID to access the Access Point, the SSID acts as a simple password and, thus, provides a measure of security. However, this minimal security is compromised if the Access Point is configured to "broadcast" its SSID. When this broadcast feature is enabled, any client computer that is not configured with a specific SSID is allowed to receive the SSID and access the Access Point. In addition, because users typically configure their own client systems with the appropriate SSIDs, they are widely known and easily shared.

While an Access Point or group of Access Points can be identified by an SSID, a client computer can be identified by the unique MAC address of its 802.11 network card. To increase the security of an 802.11 network, each Access Point can be programmed with a list of MAC addresses associated with the client computers allowed to access the Access Point. If a client's MAC address is not included in this list, the client is not allowed to associate with the Access Point.

MAC address filtering provides good security, but is best suited to small networks. Each Access Point must be manually programmed with a list of MAC addresses, and the list must be kept up to date. This administrative overhead limits the scalability of this approach.

Wireless transmissions are easier to intercept than transmissions over wired networks. To minimize this risk, the 802.11 standard specifics WEP for encryption and authentication. WEP provides encrypted communication using an encryption key between the client and an Access Point. All clients and Access Points on a wireless

network use the same key to encrypt and decrypt data. The key resides in the client computer and in each Access Point on the network. Support for WEP is standard on most current 802.11 cards and Access Points.

WEP specifies the use of a 40-bit encryption key and there are also implementations of 104-bit keys. The encryption key is concatenated with a 24-bit "initialization vector," resulting in a 64- or 128-bit key. This key is input into a pseudorandom number generator. The resulting sequence is used to encrypt the data to be transmitted.

The 802.11 standard does not specify a key management protocol, so all WEP keys on a network must be managed manually. WEP security is not available in peer-to-peer 802.11 networks that do not use Access Points.

An Access Point can be configured to provide only WEP data encryption (open-system mode) or to provide both WEP encryption and authentication (shared-key authentication. While open-system mode does not support client authentication to the Access Point, it still performs basic access control as a by-product of encrypted communications with the Access Point. In other words, if WEP is enabled and the WEP encryption key used by the client does not match the key on the Access Point, the client cannot access the network beyond the Access Point. Shared-key mode uses a shared key for authentication. Because of known security risks in implementations of shared-key authentication, open-system mode with WEP is recommended. MAC address filtering provides additional security.

While it is possible to successfully break WEP encryption, it requires time and expertise. In addition, the attacker must be close to the Access Point (within radio range). To minimize the overall exposure, our recommendation is that WEP be implemented in conjunction with MAC address filtering and SSID (with the broadcast feature disabled). We also recommend that the WEP keys be changed on a regular schedule.

MANAGING AND MONITORING TOOLS

The task of managing Access Points can be broken down into management and monitoring/reporting. Management tools are typically provided with the Access Point and should be an important consideration when selecting the Access Point vendor. Monitoring and reporting tools are typically purchased separately and provide monitoring for a wide variety of network devices, including Access Points, often using standards-based agents such as SNMP.

Management tools allow IT staff to perform initial setup and overall administration of an Access Point. Initial setup includes tasks such as configuring the device name, channel selection, SSID settings, IP addressing, security settings, and Ethernet settings. Administration includes tasks such as changing IP addresses and WEP settings, upgrading firmware, performing Access Point remote reboots, and analyzing Access Point network interfaces and Access Point client connections.

The Access Point management interface should be robust and should allow easy access to all configuration and management capabilities of the Access Point. These tools can be exposed through various interfaces such as a browser-based Web interface, command-line interface, software utility interface, and console interface. It is important to select wireless products with management tools that best meet the needs of a particular environment.

Monitoring and reporting tools can provide real-time monitoring and alerting, as well as trend reporting for wireless network devices. These tools can allow IT staff to track network device health and receive alerts of critical events or outages. IT staff can also monitor and store information over time so that longer-term network trends can be tracked and analyzed. Among other things, trend reporting is valuable when diagnosing problems and providing metrics to IT management. Purchasing high-quality monitoring and reporting tools is an integral component of any network deployment.

Additional information is available at:
www.wi-fi.com
www.enterasys.com/roamabout
http://www.nortelnetworks.com/products/01/e_lan/

KETS-SPECIFIC CONSIDERATIONS

KETS Access Points and other wireless networking components are available from Nortel Networks and Enterasys/Cabletron. These networking components have been thoroughly tested for compatibility with current KETS networking equipment and are 802.11b compliant. Wireless Access Points and other wireless networking components are to be considered no different from hard-wired networking components with regards to KETS funding. **KETS funds can only be used to purchase wireless Access Points and other wireless networking components (with the exception of wireless network cards) from KETS networking components vendors (currently Nortel Networks and Enterasys/Cabletron).**

Workstations using wireless network cards must not connect to the MUNIS financial system or the STI student management system unless using the highest possible level of security including, but not limited to, a strong SSID, WEP encryption, and MAC-address filtering. It is also recommended that administrators using the wireless network to connect to these systems use a separate Access Point with a unique strong SSID.

Wireless connections between buildings must be configured as LAN-to-LAN endpoints with a strong SSID, WEP encryption, and MAC-address filtering. Wireless WAN connectivity should be considered a temporary solution for LAN-to-LAN connectivity between buildings with large user bases due to bandwidth issues.

Channel 3 should only be used for peer-to-peer (ad-hoc) wireless networks. Channel 3 is the default for many Access Points. Please note that WEP is not available in ad-hoc mode.

When using multiple access points in close physical proximity, use channel numbers that are distant from one another. For example, if AP1 is using channel 4, then AP2 should be set to use channel 11. This eliminates the possibility of channel interference.

The use of a strong SSID is the minimum security requirement. The SSID is required to have broadcast disabled and the SSID should be at least 8 alphanumeric characters. This is referred to as a strong SSID. MAC address filtering and the use of WEP are **strongly** encouraged.

Wireless Network Cards must be able to provide at least 40-bit encryption, should be Wi-Fi certified, and conform to the 802.11b standard.